PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Title:	"System and Method for Protecting User Logoff from Web Business Transactions"		
Appellants:	Gal Ashour et al.		
Attorney Docket No.:	ARC-00-0040-US1		
Serial No.:	09/611,934	**Examiner:**	Pierre E. Elisca
Filed:	07/07/2000	**Art Unit:**	3621

Board of Patent Appeals and Interferences
Commissioner for Patents
P.O.Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Dear Sir:

This is an appeal from the Final Office Action of April 1, 2005, rejecting all the claims on file. This appeal is further to Appellants' Notice of Appeal that is attached hereto.

Table of Contents

(1) Real Party in Interest

The real party in interest is International Business Machines Corporation.

(2) Related Appeals and Interferences

No other appeals or interferences exist that relate to the present application or appeal.

(3) Status of Claims

The claims on file, namely 1, 2, 3, 5-13, and 15-17 are currently pending in the instant application. The claims on file stand rejected under 35 U.S.C. 103(a) as being unpatentable over He et al. (U. S. Pat. No. 6,088,451) hereinafter referred to as "He", in view of Barrett et al (U.S. 2001/0042051A) hereinafter referred to as "Barrett".

(4) Status of Amendments

The Final Office Action of April 1, 2005 was made in response to the amendment of February 4, 2005.

(5) Summary of Claimed Subject Matter

The present invention relates in general to a method for assisting users and institutions improve the security and resource allocation of on-line transactions. More specifically, the present invention relates to a method for protecting users conducting secure ebusiness transactions from undesirable hacking when they leave the secure sites. *(Page 1, lines 6 - 11)*

5.1. Problems addressed by the present invention

Prior to discussing the merit of the obviousness rejection under 35 U.S.C. 103, it might be desirable to review a summary of the present invention and some of the features provided thereby.

Much of the information on-line is public and accessible. However, some information is private (i.e., non-public) and access must be limited. Thus, security is of particular importance in the face of widespread hacking. Tight security is also warranted in the case of multi-user facilities where a single computer terminal is accessible to many clients. *(Page 3, line 14 - page 4, line 2).* To this end, ebusinesses implement secure user log-on and log-off functions for the exchange of this non-public information. *(Page 4, lines 10 - 11)*

In an ebusiness transaction, users seeking to access private information typically begin their transaction by first logging into a standard log-in facility. At this point they can access the secure information by providing a password or other information to the ebusiness server that identifies them as having legitimate access to given information. Ideally, the client would exchange information with the ebusiness and then log off expressly, ending the secure connection. In reality, there may be periods when the client is completely inactive but remains connected, perhaps while distracted. There may be other times when the client chooses to access another web site that is not secure. In the case of a multi-user facility such as a kiosk, the client may inadvertently leave without ending their session by logging off. In each of these cases the results are the same:

1. The client remains connected to the site even if not actively using it.
2. The client becomes prone to the theft or corruption of electronic information.
3. The ebusiness expends valuable resources maintaining a secure connection that is either under-utilized or un-utilized.
4. If the user goes to another site and then shortly thereafter returns back to the secure site, the user might not be able to reconnect before the previous session has expired or timed out. *(Page 4, line 14 - page 5, line 9).*

Periods of inactivity are unavoidable but represent a real threat to the security of the transaction. The difficulty in solving the problem lies in determining how and when a non-uniform and largely unpredictable secure session should be terminated. The problem is further complicated by the structure of the Internet and the World Wide Web. The Web's Hypertext Transfer Protocol (HTTP) is stateless, meaning that all requests for information are equivalent. No information about the client is stored during previous or even current sessions. This leaves the servers with no intrinsic information about clients or the information they have requested. *(Page 5, lines 11 - 20).*

Ebusinesses have attempted to mitigate and even solve this problem primarily though **the use of cookies**. Other implementations include embedding user information in a hidden location, or using CORBA/IIOP and JAVA RMI. Cookies are information placed on the hard disk of the client by the server to identify the user and store pertinent information about them. Typically, cookies are given a finite lifetime. In the context of secure Internet transactions, these cookies are used to log off the client

after a specified period of inactivity, and represent a second primary type of log-off, with the first being the user-initiated express log-off. *(Page 6, lines 1 - 8).*

The cookie solution for terminating sessions has several shortcomings. The fixed length of time for inactivity may result in log-offs before the client is ready to end the session. In the event that the user fails to expressly log off, the continued session may result in unauthorized access by other users. This may also extend to hackers who may take advantage of the lengthy connection times to gain access to private information. *(Page 6, lines 10 - 22).*

Prior to the advent of the present invention, there has not been an adequate mechanism by which inactive, secure Internet sessions can be terminated in an optimal way. **The use of cookies is self-limiting and inflexible, treating all users in the same manner**. There is currently no means of detecting a situation where a user may be endangering a secure transaction or private information by selecting a non-secure website while logged into a secure site. *(Page 6, lines 17 - 22.)*

5.2. Summary of the subject matter of independent claim 1

Prior to describing the subject matter of independent claim 1, it might be useful to present the definitions, in order to help in the understanding of certain terms in claim 1:

Implicit logoff: A term that is coined and defined by the inventors to mean a secure log-off procedure that can be used in addition to the conventional express log-off and cookie termination. *(Page 7, lines 3 - 6) and block 330 of FIG. 3.*

Cookie: Information supplied by a server and placed on a client's side of a client/server communication. Cookies typically reside on the client's hard disk and provide information to the server about the client. In the majority of cases, cookies have a finite lifetime. (Page 12, lines 14 - 17) *and block 330 of FIG. 3.*

The present invention is exemplified by independent claim 1, according to which a system 10 assists a user in conducting a transaction on a secure site of a server to **implicitly logoff** from the secure site. *(Page 9, lines 12 - 13).*

With Reference to FIG. 2, the server 15 includes a secure transaction protection module 115 that tracks a user's access state to the server 15. *(Page 9, lines 12 - 13).* A database 120 is in communication with the secure transaction protection module 115, for storing data to be accessed by the user. *(Page 9, lines 10 - 12).*

An identification module 110 validates the user's access to the database 120. *(Page 17, lines 4 - 8).* A notification module 150 notifies the secure transaction protection module 115 of a user's request to initiate a session on the server 15. *(Page 18, lines 12 - 17).*

If the user selects an insecure site while logged on to the secure site of the server 15, the notification module 150 sends a warning notice to the user to alert the user of an impending logoff from the secure site, and further sends a termination command to the secure transaction protection module 115 for implicitly logging off the user from the secure site. *(Page 20, lines 6 - 14).*

The secure transaction protection module 115 causes the session to be terminated in response to the termination command, absent an instruction from the user to maintain a connection with the secure site. *(Page 28, lines 17 - 19).*

The implicit log-off procedure /system 10 offers numerous advantages among which are the following:

1. The implicit log-off procedure /system 10 reduces the risks to a user resulting from choosing an insecure site while logged onto a secure site. Users are provided with pop up warnings on their monitors, alerting them to the unattended pending connection to the secure site. *(Page 7, lines 8 - 11).*

2. The implicit log-off procedure /system 10 mitigates the risk of losing control of private information as the result of a session that is not

appropriately terminated by the user. "Smart" termination by detecting inactivity during the session and the failure by the user to heed warning messages reduces the chance of hacking and/or the risk that another individual may gain terminal access to the private information. *(Page 7, lines 13 - 18).*

3. The implicit log-off procedure /system 10 mitigates the risk of losing private information as a result of a session that is terminated only after a pre-determined, universally prescribed timeout period set by a cookie. The existence of a browser with embedded "intelligence" can more exactly determine when a session should be terminated rather than having the session terminates only at the end of the cookie's predetermined time-out period. *(Page 7, line 20 - page 21, line 3).*

4. The implicit log-off procedure /system 10 reduces the business the costs associated with a non-productive, secure session. Optimally terminated transactions can reduce hardware and software costs associated with secure transactions. *(Page 8, lines 5 - 8).*

5. The implicit log-off procedure /system 10 avoids undesirable and/or unwarranted log-offs by providing to the user appropriate warnings. Users may determine their own appropriate warning/log-off period, and can avoid having a session terminated before business is complete. *(Page 8, lines 10 - 13).*

5.3. Summary of the subject matter of independent claim 9

While claim 1 exemplifies the present invention in connection with a system for assisting a user conducting a transaction on a secure site of a server to implicitly logoff from the secure site, claim 9 corresponds to claim 1, and exemplifies the present invention in connection with a computer program product for assisting a user conducting a transaction on a secure site of a server to implicitly logoff from the secure site.

5.4. Summary of the subject matter of independent claim 11

While claim 1 exemplifies the present invention in connection with a system for assisting a user conducting a transaction on a secure site of a server to implicitly logoff from the secure site, claim 11 corresponds to claim 1, and exemplifies the present invention in connection with a method for assisting a user conducting a transaction on a secure site of a server to implicitly logoff from the secure site.

(6) Grounds of Rejection to be Reviewed on Appeal

Appellants respectfully traverse the following ground of rejection and request that it be reviewed on appeal:

- Claims 1, 2, 3, 5-13, and 15-17 stand rejected under 35 U.S.C. 103(a) as being unpatentable over He et al., in view of Barrett et al. Refer to the Final Office Action of April 1, 2005 at pages 2 - 6.

(7) Arguments

7.A. The Rejection

Claims 1, 2, 3, 5-13, and 15-17 stand rejected under 35 U.S.C. 103(a) as being unpatentable over He et al. (U. S. Pat. No. 6,088,451) hereinafter referred to as "He", in view of Barrett et al (U.S. 2001/0042051A) hereinafter referred to as "Barrett". Appellants respectfully submit that neither one of the cited references discloses all the elements and limitations of the rejected claims that reflect the invention as a whole. Consequently, the claims presently on file are not obvious in view of the cited references whether considered separately or in combination with each other. In support of this position, Appellants submit the following arguments:

7.B. Legal Standard of Obviousness

The following legal authorities set the general legal standards in support of Appellants' position of non obviousness, with emphasis added for added clarity:

- MPEP 706.02(j), "**To establish a prima facie case of obviousness, three basic criteria must be met.** First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, **the prior art reference (or references when combined) must teach or suggest all the claim limitations**. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on Appellant's disclosure. In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991) ... The initial

burden is on the examiner to provide some **suggestion of the desirability** of doing what the inventor has done. "To support the conclusion that the claimed invention is directed to obvious subject matter, either the **references must expressly or impliedly suggest the claimed invention** or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references." Ex parte Clapp, 227 USPQ 972, 973 (Bd. Pat. App. & Inter. 1985)."

- **In determining the differences between the prior art and the claims, the question under 35 U.S.C. 103 is** not whether the differences themselves would have been obvious, but **whether the claimed invention as a whole would have been obvious**. The prior art perceived a need for mechanisms to dampen resonance, whereas the inventor eliminated the need for dampening via the one-piece gapless support structure. "Because that insight was contrary to the understandings and expectations of the art, the structure effectuating it would not have been obvious to those skilled in the art." 713 F.2d at 785, 218 USPQ at 700 (citations omitted).

- MPEP §2143.03, "All Claim Limitations Must Be Taught or Suggested: To establish prima facie obviousness of a claimed invention, **all the claim limitations must be taught or suggested by the prior art**. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). "**All words in a claim must be considered** in judging the patentability of that claim against the prior art." In re Wilson, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious. In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)."

- MPEP §2143.01, "The Prior Art Must Suggest The Desirability Of The Claimed Invention: There are three possible sources for a motivation to combine references: the nature of the problem to be solved, the teachings of the prior art, and the knowledge of persons of ordinary skill in the art." In re Rouffet, 149 F.3d 1350, 1357, 47 USPQ2d 1453, 1457-58 (Fed. Cir. 1998) (**The combination of the references taught every element of the claimed invention, however without a motivation to combine, a rejection based on a prima facie case of obvious was held improper**.). The level of skill in the art cannot be relied upon to provide the suggestion to combine references. Al-Site Corp. v. VSI Int'l Inc., 174 F.3d 1308, 50 USPQ2d 1161 (Fed. Cir. 1999).

- "**Obviousness cannot be established** by combining the teachings of the prior art to produce the claimed invention, **absent some teaching or suggestion** supporting the combination." *In re Fine, 837 F.2d at 1075, 5 USPQ2d at 1598* (citing *ACS Hosp. Sys. v. Montefiore Hosp., 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984)).* **What a reference teaches** and whether it teaches toward or **away from the claimed invention** are questions of fact. See *Raytheon Co. v. Roper Corp., 724 F.2d 951, 960-61, 220 USPQ 592, 599-600 (Fed. Cir. 1983),* cert. denied, *469 U.S. 835, 83 L. Ed. 2d 69, 105 S. Ct. 127 (1984).* "

- "When a rejection depends on a combination of prior art references, there must be **some teaching, suggestion, or motivation** to combine the references. See *In re Geiger,* 815 F.2d 686, 688, 2 USPQ2d 1276, 1278 (Fed. Cir. 1987)." Obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention **where there is some teaching, suggestion, or motivation** to do so found either explicitly or implicitly in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See MPEP 2143.01; In re Kotzab, 217 F.3d 1365, 1370, 55 USPQ2d 1313, 1317 (Fed. Cir. 2000); In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); and In re Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992).

- "With respect to core factual findings in a determination of patentability, however, the **Board cannot simply reach conclusions based on its own understanding or experience** -- or on its assessment of what would be basic knowledge or common sense. **Rather, the Board must point to some concrete evidence in the record** in support of these findings." See In re Zurko, 258 F.3d 1379 (Fed. Cir. 2001).

- "We have noted that **evidence of a suggestion, teaching, or motivation to combine** may flow from the prior art references themselves, the knowledge of one of ordinary skill in the art, or, in some cases, from the nature of the problem to be solved, see Pro-Mold & Tool Co. v. Great Lakes Plastics, Inc., 75 F.3d 1568, 1573, 37 USPQ2d 1626, 1630 (Fed. Cir. 1996), Para-Ordinance Mfg. v. SGS Imports Intern., Inc., 73 F.3d 1085, 1088, 37 USPQ2d 1237, 1240 (Fed. Cir. 1995), although "the suggestion more often comes from the teachings of the pertinent references," Rouffet, 149 F.3d at 1355, 47 USPQ2d at 1456. The range of sources available, however, does not diminish the requirement for actual evidence. That is, **the showing must be clear and particular**. See, e.g.,

C.R. Bard, 157 F.3d at 1352, 48 USPQ2d at 1232. **Broad conclusory statements regarding the teaching of multiple references, standing alone, are not "evidence."** E.g., McElmurry v. Arkansas Power & Light Co., 995 F.2d 1576, 1578, 27 USPQ2d 1129, 1131 (Fed. Cir. 1993) ("Mere denials and conclusory statements, however, are not sufficient to establish a genuine issue of material fact."); In re Sichert, 566 F.2d 1154, 1164, 196 USPQ 209, 217 (CCPA 1977)." See In re Dembiczak, 175 F. 3d 994 (Fed. Cir. 1999).

- "To prevent the use of hindsight based on the invention to defeat patentability of the invention, **this court requires the examiner to show a motivation to combine the references** that create the case of obviousness. In other words, **the examiner must show reasons** that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would select the elements from the cited prior art references **for combination in the manner claimed**." See In re Rouffet, 149, F.3d 1350 (Fed. Cir. 1998).

- The mere fact that references can be combined or modified does not render the resultant combination obvious **unless the prior art also suggests the desirability of the combination**. In re Mills, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990). Although a prior art device "may be capable of being modified to run the way the apparatus is claimed, **there must be a suggestion or motivation in the reference** to do so." 916 F.2d at 682, 16 USPQ2d at 1432.). See also In re Fritch, 972 F.2d 1260, 23 USPQ2d 1780 (Fed. Cir. 1992) (flexible landscape edging device which is conformable to a ground surface of varying slope not suggested by combination of prior art references).

- If the **proposed modification would render the prior art invention being modified unsatisfactory** for its intended purpose, then there is no suggestion or motivation to make the proposed modification. In re Gordon, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984).

7.C. Application of the Obviousness Standard to the Present Invention

The following Table summarizes Appellants' arguments in response to the Final Office Action, in support of the allowability of the representative independent claim 1.

CLAIM 1	OFFICE ACTION REJECTION GROUNDS	ARGUMENTS
1. A system for assisting a user conducting a transaction on a secure site of a server to **implicitly logoff from the secure site**, comprising: the server including:	As per claims 1, 2, 3, 5-13 and 15-17 He discloses a system/method for securing access to network elements by user elements, wherein the network elements and the user elements are coupled to a network. A network security server ... comprising: the server including:	(7.C.1) He does not disclose an implicit logoff process.
a secure transaction protection module that tracks a user's access state to the server;	a secure transaction protection module that tracks a user's access state to the server (see., abstract, lines 7-13, fig 2, please note that user credentials or privileges also include Web site);	
a database in communication with the secure transaction protection module, for storing data to be accessed by the user;	a database in communication with the secure transaction protection module, for storing data to be accessed by the user (see., abstract, lines 14-16, col 2, lines 12-34);	
an identification module for validating the user's access to the database; and	an identification module for validating the user's access to the database (see., abstract, line 7-13, col 2, lines 12-34); and	
a notification module for notifying the secure transaction protection module of a user's request to initiate a session on the server;	a notification module for notifying the secure transaction protection module of a user's request to initiate a session on the server (see., col 31, lines 30-38).	

wherein if the user selects an insecure site while logged on to the secure site of the server, the notification module sends a warning notice to the user to alert the user of an impending logoff from the secure site, **and further sends a termination command** to the secure transaction protection module for implicitly logging off the user from the secure site; and wherein the secure transaction protection module **causes the session to be terminated** in response to the termination command, absent an instruction from the user to maintain a connection with the secure site.	**It is to be noted that He does not explicitly disclose wherein if the user selects site while logged on to the secure site of the server, the notification module sends a warning notice to the user to alert the user of an impending logoff from the secure site, and further sends a termination command to the secure transaction protection module for implicitly logging off** (implicit logging off or leaving the secure site) **the user from the secure site, and wherein response to the termination command, absent an instruction from the user to maintain a connection with the secure site exists the secure site, the notification module sends a message to the secure transaction protection module for logging off the user from the secure site.** However, Barrett discloses web browsers that require that a security warning be displayed to the user which indicates that the user is leaving a secured communication channel (see **page 5, col 1, lines 21-48**). Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the security system of He by including the limitations detailed above as taught by Barrett because such modification would provide the security system of He with the enhanced capability of notifying when a user exists the central controller or (secure site).	(7.C.2) Neither He nor Barrett provides for an "implicit logoff" process as claimed. (7.C.3) Neither He nor Barrett provides the ability to allow the "implicitly log off" process to terminate the connection absent a user instruction to the contrary. (7.C.5) He and Barrett cannot be properly combined.

7.C.1. He does not disclose an implicit logoff process.

He does not disclose an implicit logoff process. Appellants have already provided a specific definition of the concept of "implicit logoff" to include a secure log-off procedure **that can be used in addition to** the conventional express log-off and cookie termination.

More specifically, the term "implicit log-off" was coined in the instant application for the purpose of describing the functionality of the invention, as follows: "implicit log-off (at step 330, which) means that the client will implicitly send the log-off message event to the server 15 **without the user explicitly choosing the logout option**."

Since the term "implicit log-off" was clearly defined by Appellants, it would not be permissible for the Examiner to redefine this term in hind-sight, in order to justify a rejection ground. As an example, the fact that the user has left the initial site and the central controller is notified, does not imply that the user will be automatically and implicitly logged off, as described in the present application.

7.C.2. Neither He nor Barrett provides for an "implicit logoff" process as claimed

Appellants agree with the Examiner that He does not explicitly disclose:

(1) wherein if the user selects an insecure site while logged on to the secure site of the server, the notification module sends a warning notice to the user to alert the user of an impending logoff from the secure site, and

(2) further sends a termination command to the secure transaction protection module for implicitly logging off the user from the secure site, and further sends a termination command to the secure transaction protection

module for implicitly logging off (implicit logging off or leaving the secure site) the user from the secure site, and

(3) where in response to the termination command, absent an instruction from the user to maintain a connection with the secure site exists the secure site, the notification module sends a message to the secure transaction protection module for logging off the user from the secure site.

In essence, the Examiner is basically arguing that the main reference, namely **He, does not disclose the foregoing important elements of the present invention**. Rather, the Examiner resorts to a secondary reference, Barrett, to compensate for the absence of these elements.

7.C.3. Neither He nor Barrett provides the ability to allow the "implicitly log off" process to terminate the connection absent a user instruction to the contrary.

The Examiner states that Barrett discloses web browsers that require that a security warning be displayed to the user which indicates that the user is leaving a secured communication channel, and refers to **page 5, col 1, lines 21-48** (Paragraph 47) of Barrett. However, Paragraph 47 states in part, as follows, with emphasis added:

> "**The user cannot actually leave the secured communication channel until clicking the "continue" button on the security warning**. This extra step imposes an additional burden on the consumer and slows down the processing of the transaction."

In other terms, contrary to the present invention, the Barrett system does not automatically leave the secure site, until expressly authorized by the user. **This feature**, which is relied upon by the Examiner, actually **teaches away from the present invention that teaches "implicit logoff"** to terminate the connection.

7.C.4. The Examiner failed to establish a prima facie case of obviousness.

The Examiner resorts to Barrett as disclosing a security warning. **However, the Examiner does not address the following remaining features**, which, admittedly (by the Examiner) are not disclosed by the primary reference, He:

> "the notification module sends a warning notice to the user to alert the user of an impending logoff from the secure site, **and further sends a termination command** to the secure transaction protection module for implicitly logging off the user from the secure site; and
>
> wherein the secure transaction protection module **causes the session to be terminated** in response to the termination command, absent an instruction from the user to maintain a connection with the secure site."

Appellants respectfully submit that the foregoing two claim elements are neither disclosed by He nor by Barrett. Accordingly, and pursuant to MPEP 706.02(j) that states: "To establish a prima facie case of obviousness, three basic criteria must be met ... the prior art reference (or references when combined) must teach or suggest all the claim limitations," since **neither He nor Barrett discloses all the elements/limitations of claim 1, the Examiner failed to establish a prima facie case of obviousness.**

7.C.5. He and Barrett cannot be properly combined.

Appellants submit that He and Barrett cannot be properly combined in view of the legal grounds above. Neither nor Barrett provides evidence of a suggestion, teaching, or motivation to combine these two references. The legal authorities above require that the evidence be clear and particular, and note that broad conclusory statements regarding the teaching of multiple references, standing alone, are not "evidence."

More specifically, the fact that it would be desirable to combine "two" references, neither of which teaches the important elements of the invention as claimed, simply to "provide the security system of He with the enhanced capability of notifying when a user exists the central controller or (secure site)" does not qualify as "evidence" within the ambit of the legal authorities above. Actually, it should be clear that the present invention relates to "implicit logoff, and none of these two references provides the ability to allow the "implicitly log off" process to terminate the connection absent a user instruction to the contrary. In addition, and as indicated earlier, Barrett teaches away from the implicit logoff concept and thus clearly distinguishes over claim 1 of the present invention.

In response to this argument, the Examiner cited several legal authorities in support of the combination of the references, and further presented the following counter-arguments:

> "Applicant also argues that the implicit log-off reduces the risk to a user resulting from choosing an insecure site while logged onto a secure site". As indicated above, **Barrett discloses web browsers that require that a security warning be displayed to the user which indicates that the user is leaving a secured communication channel**. This process is readable as when a user leaving a secure site, a security warning be displayed to the user which indicates that the user is visiting a insecure site (see page 5, col 1, lines 21-48). Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the security system of He by including the limitations detailed above as taught by Barrett because such modification would provide the security system of He with the enhanced capability of notifying when a user exists the central controller or (secure site)." Emphasis added.

In essence, the Examiner has totally ignored the gist of the present invention (as recited in claim 1), in that the present system "**sends a termination command** to the secure transaction protection module for implicitly logging off the user

from the secure site; and wherein the secure transaction protection module **causes the session to be terminated** in response to the termination command."

The Examiner's argument is irrelevant to the present invention in that an important aspect of the present invention is that the session be terminated pursuant to the implicit logoff process (as defined by the inventors). Contrary to the Examiner's position, the warning messages that could be displayed to the user are irrelevant as they do not automatically terminate the session pursuant to the implicit logoff process of the present invention.

As a result, claim 1 is not obvious in view of He or Barrett, and the allowance of this claim and the claims dependent thereon is earnestly solicited.

Independent claims 9 and 11 are allowable for containing a similar subject matter to that of claim 1. Therefore, claims 9 and 11 and the claims dependent thereon are also allowable.

Appellants respectfully request that all the claims on file be allowed.

Respectfully submitted,

Date: July 12, 2005

Samuel A. Kassatly Law Office
20690 View Oaks Way
San Jose, CA 95120
Tel.: (408) 323-5111
Fax: (408) 521-0111

Samuel A. Kassatly
Attorney for Appellants
Reg. No. 32,247

APPENDIX A

CLAIMS ON APPEAL

1. A system for assisting a user conducting a transaction on a secure site of a server to implicitly logoff from the secure site, comprising:

the server including:

a secure transaction protection module that tracks a user's access state to the server;

a database in communication with the secure transaction protection module, for storing data to be accessed by the user;

an identification module for validating the user's access to the database; and

a notification module for notifying the secure transaction protection module of a user's request to initiate a session on the server;

wherein if the user selects an insecure site while logged on to the secure site of the server, the notification module sends a warning notice to the user to alert the user of an impending logoff from the secure site, and further sends a termination command to the secure transaction protection module for implicitly logging off the user from the secure site; and

wherein the secure transaction protection module causes the session to be terminated in response to the termination command, absent an instruction from the user to maintain a connection with the secure site.

2. (Canceled)

3. The system according to claim 1, wherein the secure transaction protection module provides the user with an option to set the time to termination.

4. The system according to claim 1, wherein the secure transaction protection module sends a cookie with a short life to the notification module to terminate the session following the expiration of the cookie.

5. The system according to claim 1, wherein the secure site is a web site with an address; and

wherein the user exits the secure site by transiting to another address.

6. The system according to claim 1, wherein the transaction is an ebusiness transaction.

7. The system according to claim 6, wherein the user accesses the secure site using a web browser.

8. The system according to claim 7, wherein the notification module is implemented on the web browser.

9. A computer program product for assisting a user conducting a transaction on a secure site of a server to implicitly logoff from the secure site, comprising:

the server including:

a secure transaction protection module that tracks a user's access state to the server;

a database in communication with the secure transaction protection module, for storing data to be accessed by the user;

an identification module for validating the user's access to the database; and

a notification module for notifying the secure transaction protection module of a user's request to initiate a session on the server;

wherein if the user selects an insecure site while logged on to the secure site of the server, the notification module sends a warning notice to the user to alert the user of an impending logoff from the secure site, and further sends a termination command to the secure transaction protection module for implicitly logging off the user from the secure site; and

wherein the secure transaction protection module causes the session to be terminated in response to the termination command, absent an instruction from the user to maintain a connection with the secure site.

10. The computer program product according to claim 9, wherein the secure transaction protection module provides the user with an option to set the time to termination.

11. A method for implicitly logging off a user conducting a transaction on a secure site of a server from the secure site, comprising:

tracking a user's access state to the server;

storing data to be accessed by the user;

validating the user's access to the database;

notifying the secure transaction protection module of a user's request to initiate a session on the server;

wherein if the user selects an insecure site while logged on to the secure site of the server, sending a warning notice to the user to alert the user of an impending logoff from the secure site, and further issuing a termination command to the secure transaction protection module for implicitly logging off the user from the secure site; and

causing the session to be terminated in response to the termination command, absent an instruction from the user to maintain a connection with the secure site.

12. (Canceled)

13. The method according to claim 11, further comprising providing the user with an option to set the time to termination.

14. The method according to claim 11, wherein issuing the command includes sending a cookie with a short life to the notification module to terminate the session following the expiration of the cookie.

15. The method according to claim 11, wherein exiting the secure site includes transiting to another site.

16. The method according to claim 11, further including performing an ebusiness transaction.

17. The method according to claim 16, wherein accessing the secure site includes using a web browser.

==========